UNIVERSIDAD POLITÉCNICA DE

SAN LUIS POTOSÍ

CARRERA: Ingeniería en Tecnologías de la Información

MATERIA: Seguridad Informática

TRABAJO:Actividad 05 Pentesting

PARCIAL 1

Aguilar Carrizales Miguel Angel / 182318

Fecha de entrega: 16 de Febrero de 2026

Introducción

La seguridad informática es un pilar fundamental en la protección de sistemas, aplicaciones y datos frente a amenazas cada vez más sofisticadas. Para evaluar de manera efectiva el nivel de exposición y resiliencia de una organización, se emplean metodologías de prueba de penetración y marcos de evaluación estandarizados. Estas metodologías permiten identificar vulnerabilidades, simular ataques reales y establecer planes de mitigación basados en buenas prácticas reconocidas internacionalmente.

En está tabla comparativa se revisará la información de MTRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES, ISSAF.

En conjunto, estas metodologías ofrecen un enfoque sistemático y complementario para detectar debilidades, medir riesgos y fortalecer la postura de seguridad de cualquier organización. Su aplicación no solo ayuda a cumplir con normativas y estándares, sino que también fomenta una cultura de prevención y resiliencia frente a ciberataques.

Metodología	Descripción breve	Fases de implementación	Objetivo principal	Escenarios de uso	Orientación	Autor/Organismo	URL oficial	Certificaciones	Vigencia / Actualización
MITRE ATT&CK	Base de conocimiento que clasifica tácticas y técnicas usadas por atacantes reales. No es guía de pentesting paso a paso, sino marco de referencia de comportamiento adversario.	1. Reconocimiento de amenazas 2. Mapeo de técnicas 3. Simulación/red teaming 4. Evaluación de cobertura defensiva	Identificar, modelar y detectar técnicas de ataque reales.	SOC, Blue Team, Red Team, Threat Hunting, análisis post-incidente.	Evaluación y defensa	MITRE Corporation	https://attack.mitre.org	*ATT&CK Fundamentals*, *Threat Intelligence*, *Detection Engineering* y *Purple Teaming*.	2025, actualización continua
OWASP WSTG	Guía de pruebas de seguridad para aplicaciones web basada en riesgos. Estándar práctico para pentesting web.	1.Antes de que comience el desarrollo 2. Durante la definición y el diseño 3, Durante el desarrollo	Detectar vulnerabilidades en aplicaciones web.	Web apps, APIs, comercio electrónico, fintech.	Ataque, evaluación	OWASP Foundation	OWASP Web Security Testing Guide	No posee una certificación directa	Versión 4.2

		4.Durante la implementación/ despliegue 5. Durante el mantenimiento y las operaciones							
NIST SP 800-115	Guía técnica del gobierno de EE.UU. para pruebas de seguridad y evaluación de controles.	Despliegue – Mantenimiento y Operaciones	Evaluar controles de seguridad organizacionales.	Entornos gubernamentales, corporativos, auditorías formales.	Evaluación y ataque	NIST (National Institute of Standards and Technology)	https://csrc.nist.gov/publications/detail/sp/800-115/final	CISSP, CISA (alineadas a NIST)	Publicado 2008
OSSTMM	Metodología científica para medir seguridad operativa. Se enfoca en métricas y objetividad.	1. Preparación 2. Recolección de información 3. Análisis de superficie de ataque 4. Métricas y reporte	Medir seguridad de forma cuantificable.	Infraestructura, redes, telecomunicaciones, físico.	Evaluación	ISECOM	https://www.isecom.org/OSSTMM.3.pdf	OPSA (OSSTMM Professional Security Analyst) y OPST (OSSTMM Professional Security Tester)	Versión 3.0.2

PTES	Marco práctico para estructurar pruebas de penetración de inicio a fin.	1.Pre-engagement 2. Inteligencia 3. Modelado de amenazas 4. Análisis de vulnerabilidades 5. Explotación 6Post-explotación 7. Reporte	Estandarizar el proceso completo de pentesting.	Empresas privadas, consultoría, auditorías externas.	Ataque y evaluación.	PTES Technical Guidelines	http://www.pentest-standard.org	No tiene certificación directa	2014
ISSAF	Marco detallado de pruebas técnicas estructuradas por dominio de seguridad.	Definición y Diseño – Despliegue – Mantenimiento y Operaciones	Evaluar seguridad en múltiples capas.	Redes corporativas, servidores, infraestructura TI.	Ataque y evaluación.	OISSG (Open Information Systems Security Group)	http://www.oissg.org/issaf	No cuenta con certificación directa	Última publicación en 2006

Conclusión

Las metodologías de prueba de penetración y evaluación de la seguridad informática como MITRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES e ISSAF representan enfoques complementarios que permiten a las organizaciones enfrentar el reto de proteger sus activos digitales en un entorno de amenazas en constante evolución. Cada marco aporta una perspectiva distinta: desde el análisis de tácticas y técnicas de atacantes, hasta guías prácticas de pruebas en aplicaciones web, estándares de ejecución de pentesting y evaluaciones integrales de sistemas.

La aplicación de estas metodologías no debe entenderse como esfuerzos aislados, sino como piezas de un ecosistema de seguridad que, al integrarse, ofrecen una visión más completa y robusta.